CLEARTEXT CREDENTIALS

Leslie Martinez | 05Dec2025

Challenge: CLEARTEXT CREDENTIALS - CRITICAL SEVERITY

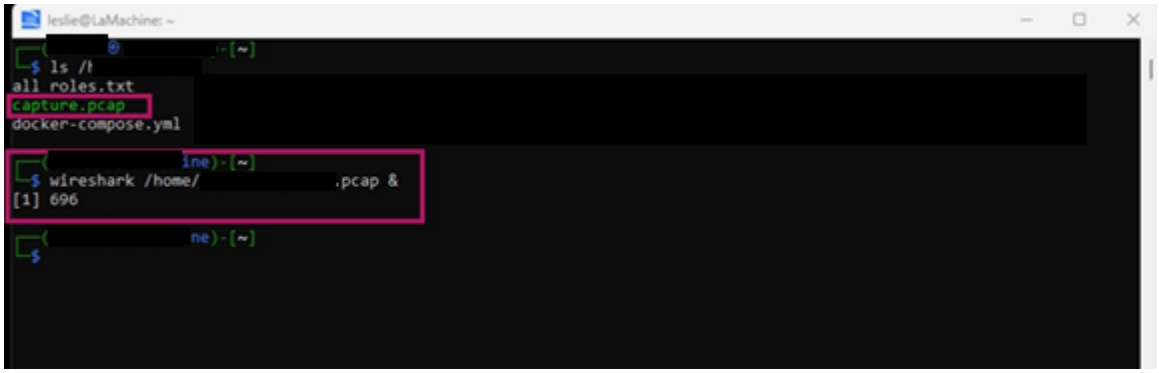
CWE-319: Cleartext Transmission of Sensitive Information
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

SUMMARY

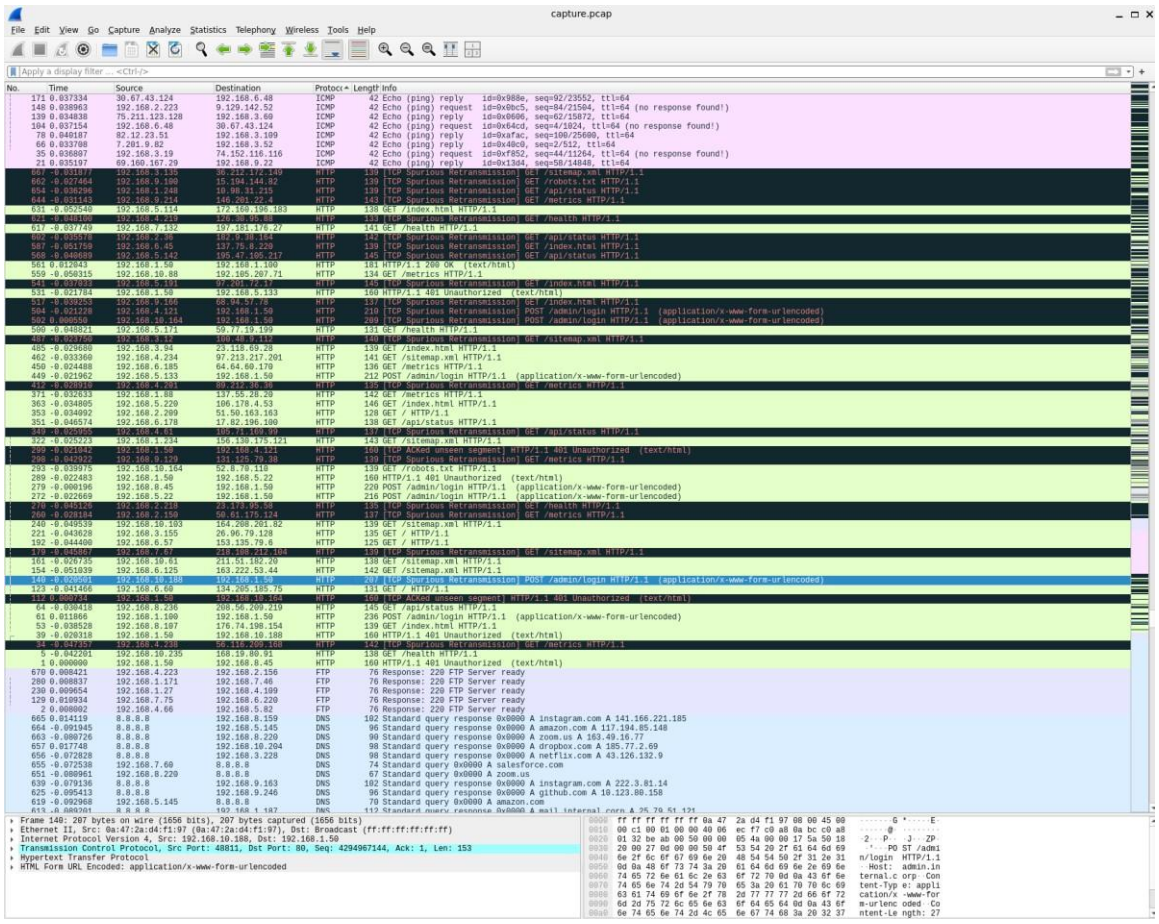
A packet capture file had threat activity and after inspecting the http requests that a user was logging into an internal administrative login portal. I reviewed the captured traffic with Wireshark, and the authentication credentials were transmitted in cleartext using URLencoded form data. There is a lack of transport-layer security enabled in which it compromised the login by simply inspecting the captured POST request.

STEPS TO REPRODUCE

1. Load the pcap file
   I downloaded the file from the site and opened it with Wireshark for inspection

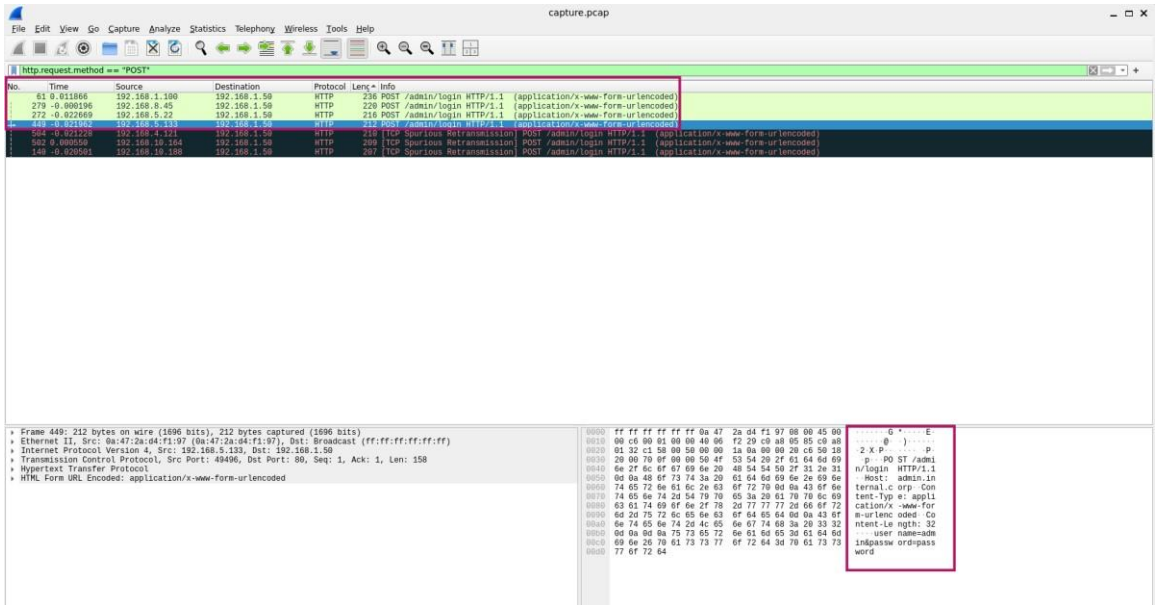


2. Sort through the packet files
   Sorting the packets by protocol allowed me to review the information in a clearer view to spot any activity that is out of the ordinary

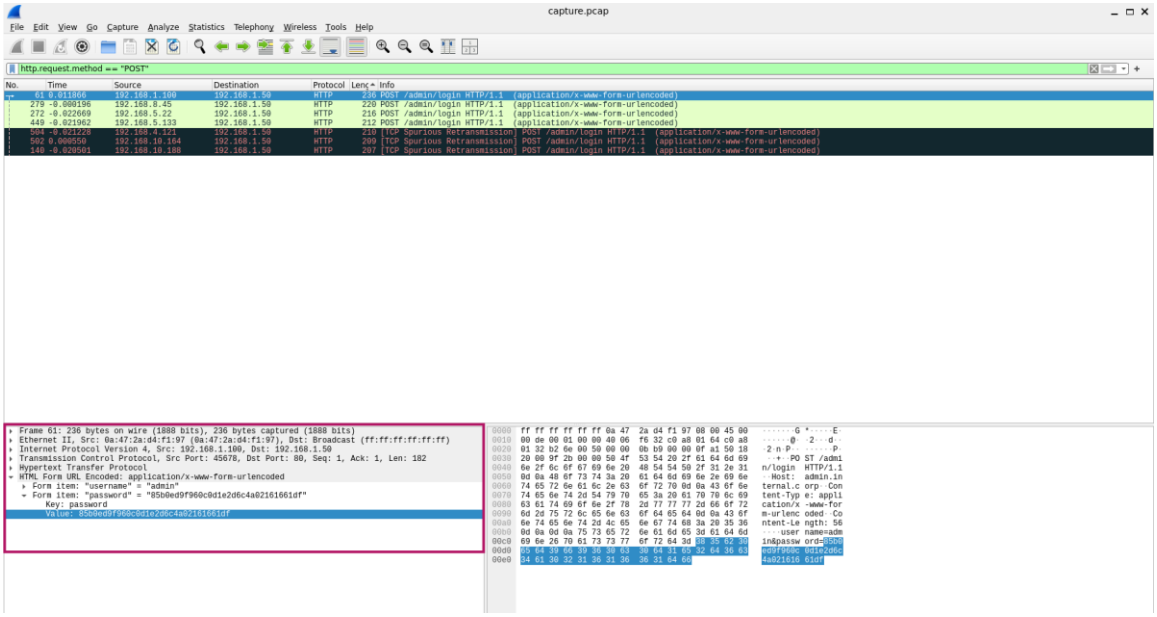


3. Identify and filter the files

   After reviewing the packet files, I noticed multiple http transactions were occurring in the internal admin portal



4. Extract the credentials
   Inspecting each POST I was able to see the username and password form item visible, identifying the successful post with the 200 POST the password was a 32charcter hex that doubled as the flag



REMEDIATION STEPS

- Enforce HTTPS/TLS for authentication endpoints to safeguard user credentials
- Avoid transmitting plaintext passwords and token-based authentication
- Prevent use of direct credential submissions without encryption
- Apply network segmentation to limit attackers from capturing internal traffic

REFERENCES

- NVD - CVE-2022-46680
- CWE - CWE-319: Cleartext Transmission of Sensitive Information (4.18)
- M3: Insufficient Transport Layer Protection | OWASP Foundation
- ICS Communications: Frail Security in Protocols | Martello Security